Web Applications & APIs

The Soft Belly of the Cloud

Dave Ferguson
Director of Product Management, WAS

Remi Le Mer
Director of Product Management, WAF

Agenda

Web Apps & APIs in the Cloud

Qualys Web Application Scanning

    Review

    What's New

    Roadmap

Qualys Web Application Firewall

    Review

    What's New

    Roadmap

Q&A

Qualys.

Insecure Apps & APIs are a Problem

Your business depends on web applications

Any app or API can be a foothold into your organization

Developers are not incentivized for security
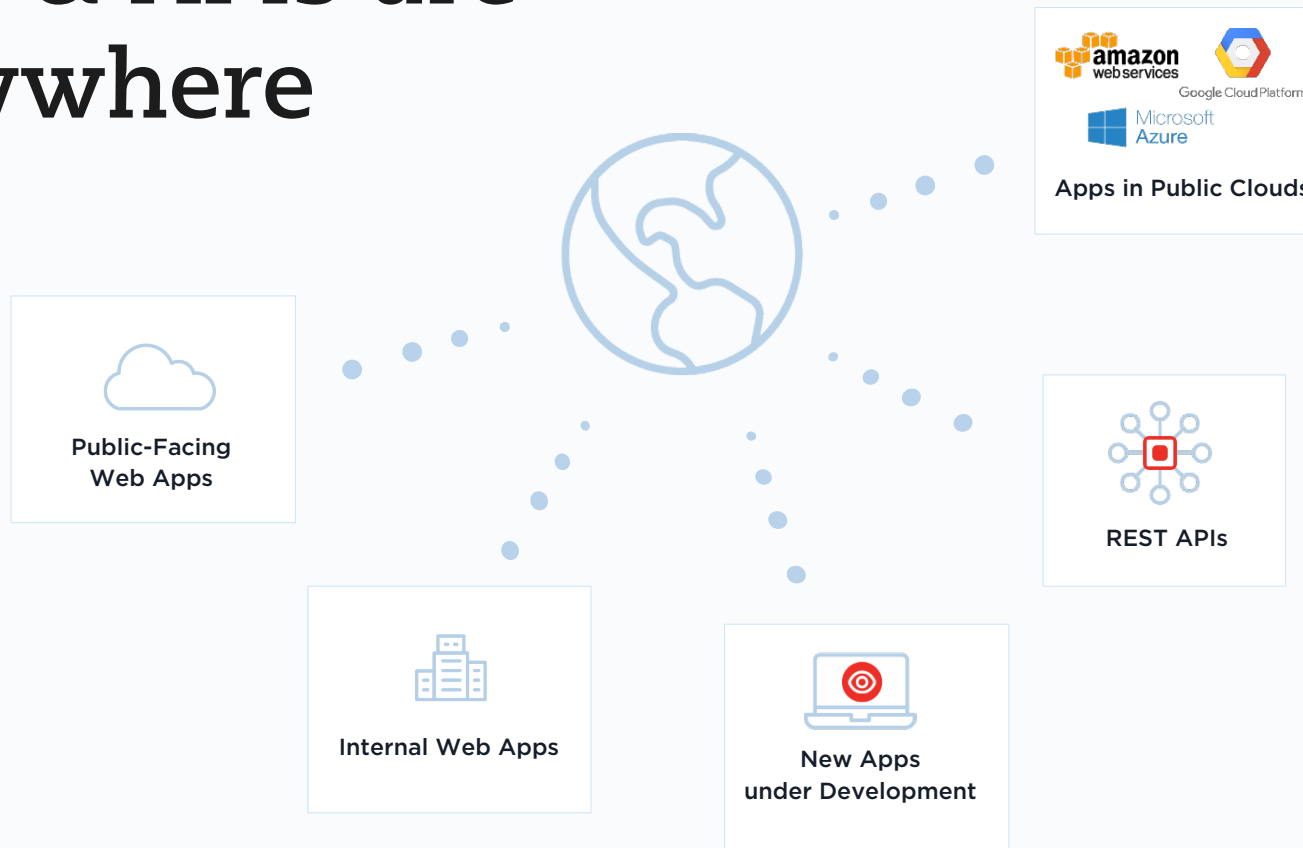
Cloud-based apps are easy for developers to deploy

Web Applications are Being Targeted

➢ Most common data breach pattern *

➢ Top hacking vector *

Panera Bread	2018
Facebook (API)	2018
Google+ (API)	2018
MyFitnessPal (API?)	2017
Equifax	2017
Yahoo	2016
Ashley Madison	2015
OPM	2015

* Source: 2018 Verizon DBIR

Apps & APIs are Everywhere

Apps in Public Clouds

Public-Facing Web Apps

REST APIs

Internal Web Apps

New Apps under Development

Qualys.

Web Application Scanning

Review

Qualys WAS

A leading dynamic application security testing (DAST) tool

Delivered via the Qualys Cloud Platform

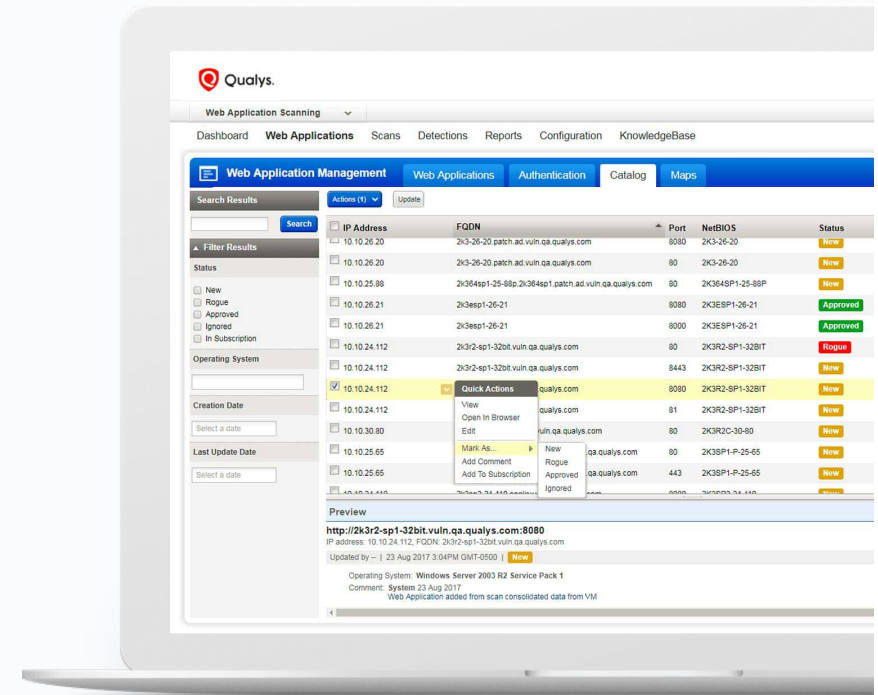Identifies app-layer vulnerabilities
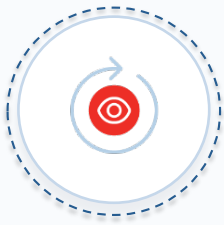
- OWASP Top 10
- CWEs
- Web-related CVEs

Includes automated crawling

Supports Selenium scripts

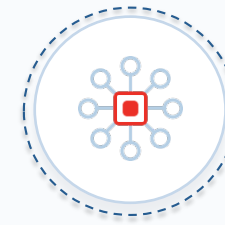Malware monitoring as a bonus

Qualys.

Built for the Enterprise

Web App Discovery
Unlimited scans &
users
RBAC
Tagging

Scheduled scans
Ad-hoc, targeted
scans
Multi-site scans
Retest vulnerability
Scan for malware

Massive scalability
Detection history
Scheduled reports
Customizable
reports
Swagger support

Robust API
CI/CD integration
Unique integration
w/Qualys WAF
Bi-directional
integration with
Bugcrowd

Qualys.

What's New in Qualys WAS

Scanning REST APIs

https://
swagger.io

https://
www.openapis.org

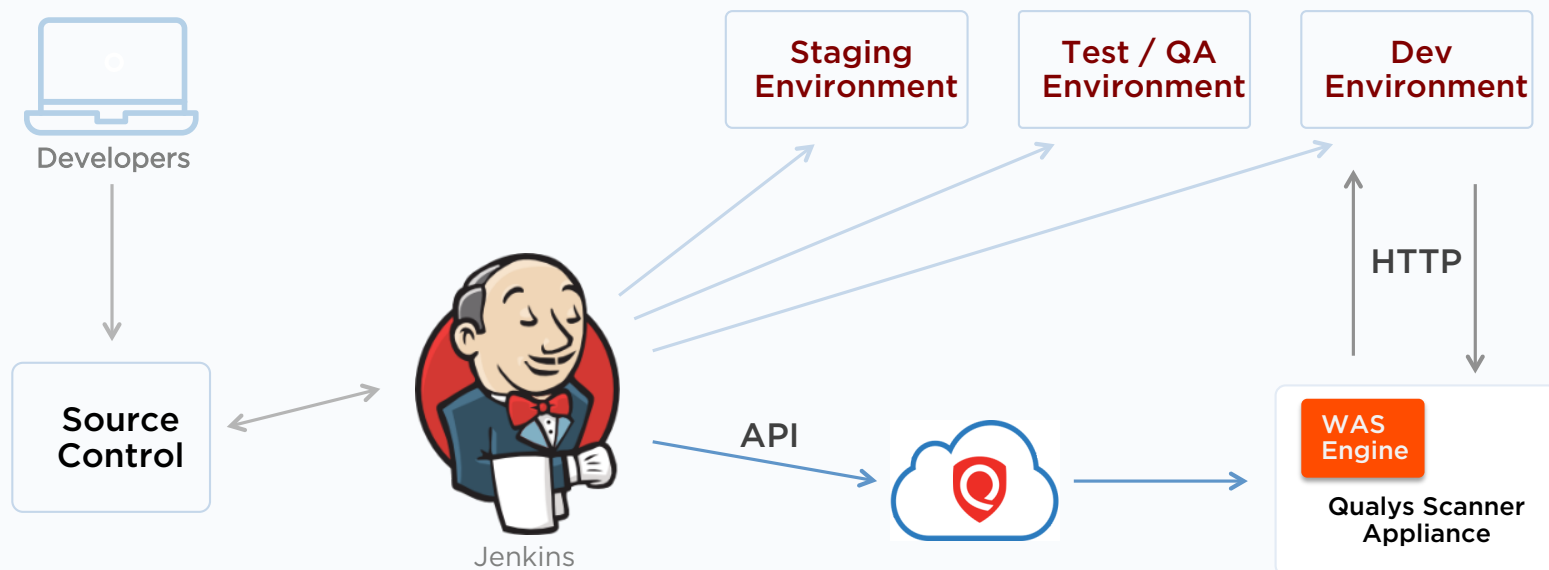Swagger is specification that describes a set of REST APIs

Swagger file typically available from dev team
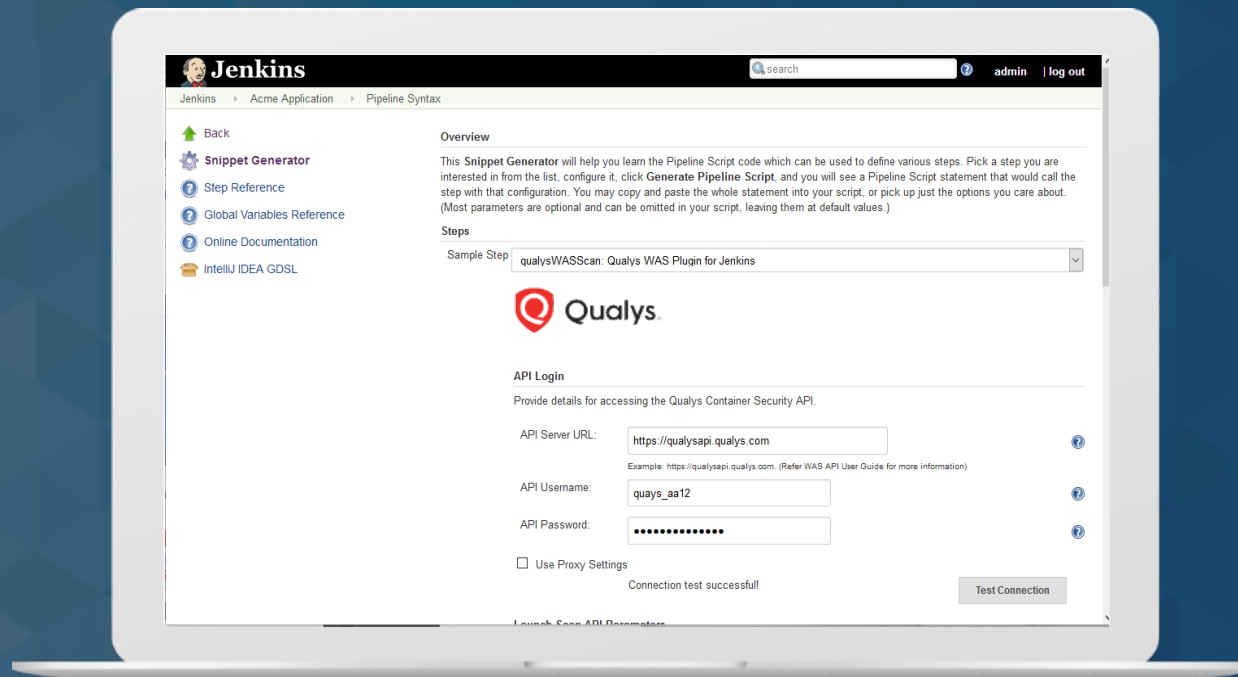
Set Swagger file as target URL in Qualys WAS

API endpoints are automatically tested for vulnerabilities

Swagger v2 JSON format currently supported

Qualys.

Automate Scans in CI/CD with Qualys WAS

Developers

Source Control

Jenkins

API

Staging Environment

Test / QA Environment

Dev Environment

HTTP

WAS Engine

Qualys Scanner Appliance

Qualys.

Jenkins Plugin for WAS

Manual Testing Complements WAS

Dynamic application testing is one piece of the AppSec puzzle

Manual penetration testing important for your business-critical apps

Qualys WAS offers:

      Bugcrowd integration

      Burp Suite integration

      Partnerships with consulting shops

Qualys.

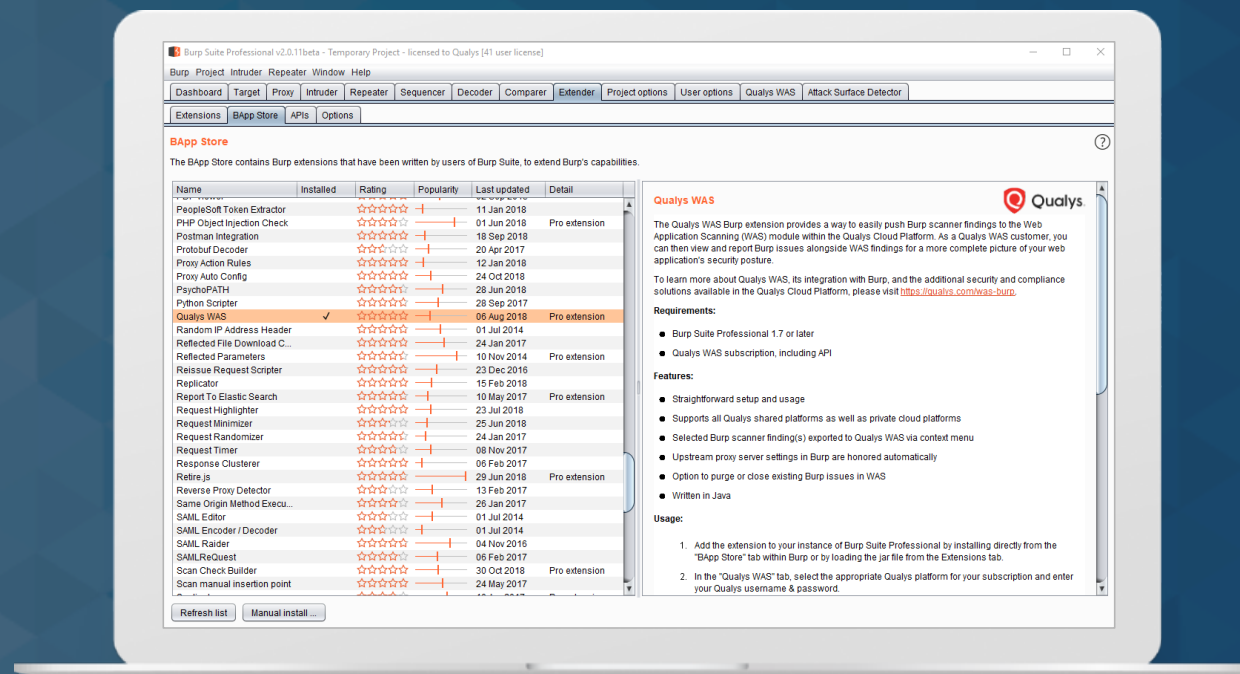# Bi-directional Integration with Bugcrowd

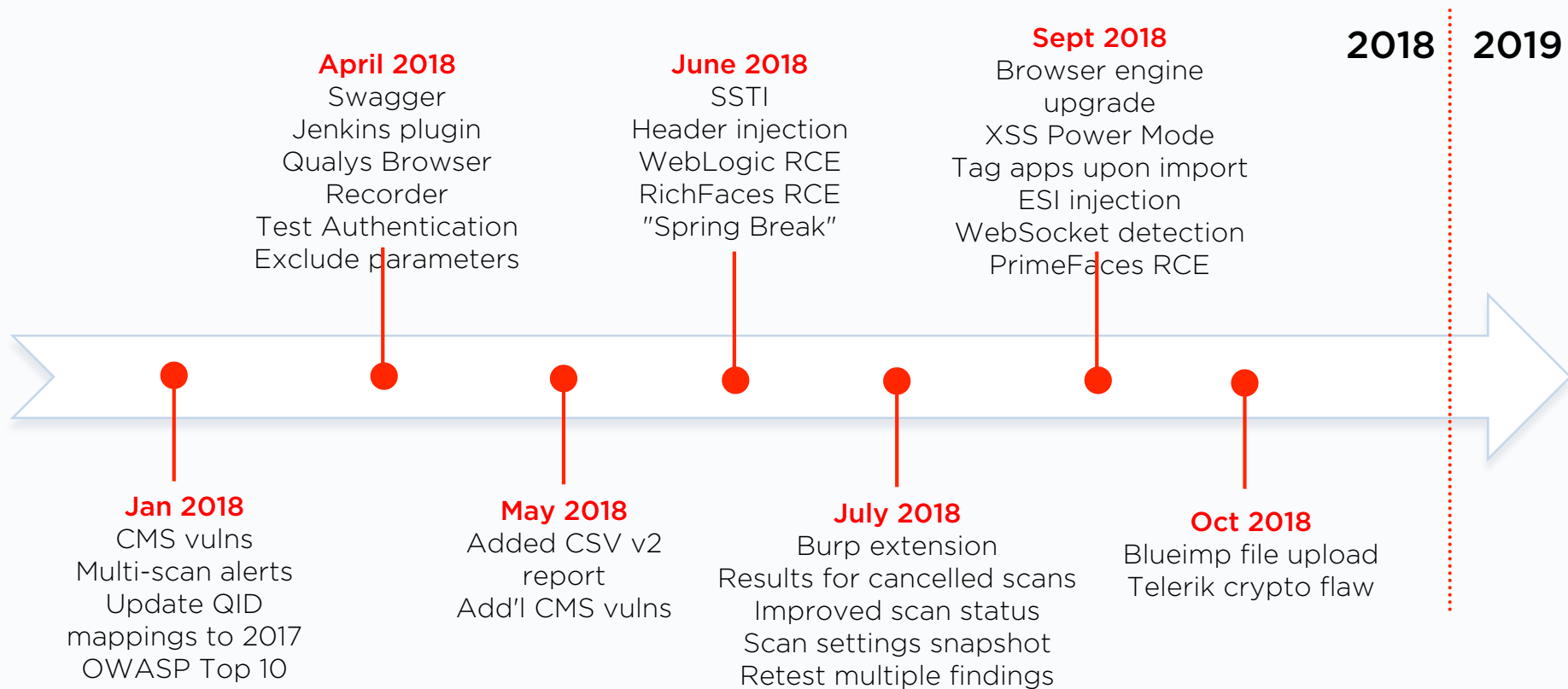# Qualys WAS Burp Extension

Burp Suite

Web Application Scanning

A quick, intuitive way to send Burp-discovered issues into WAS
Provides centralized viewing/reporting of WAS detections + Burp issues
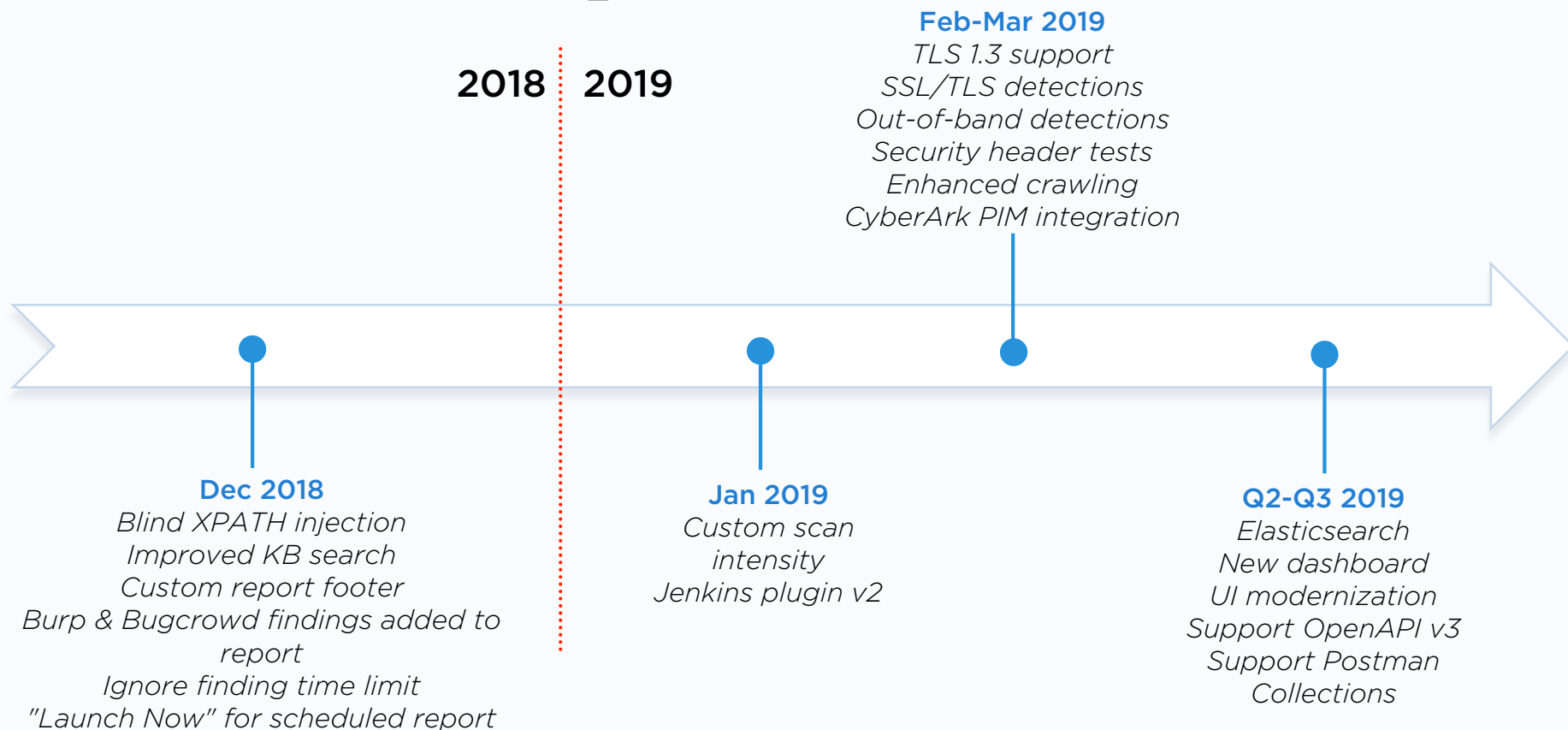
Available in Burp's BApp Store
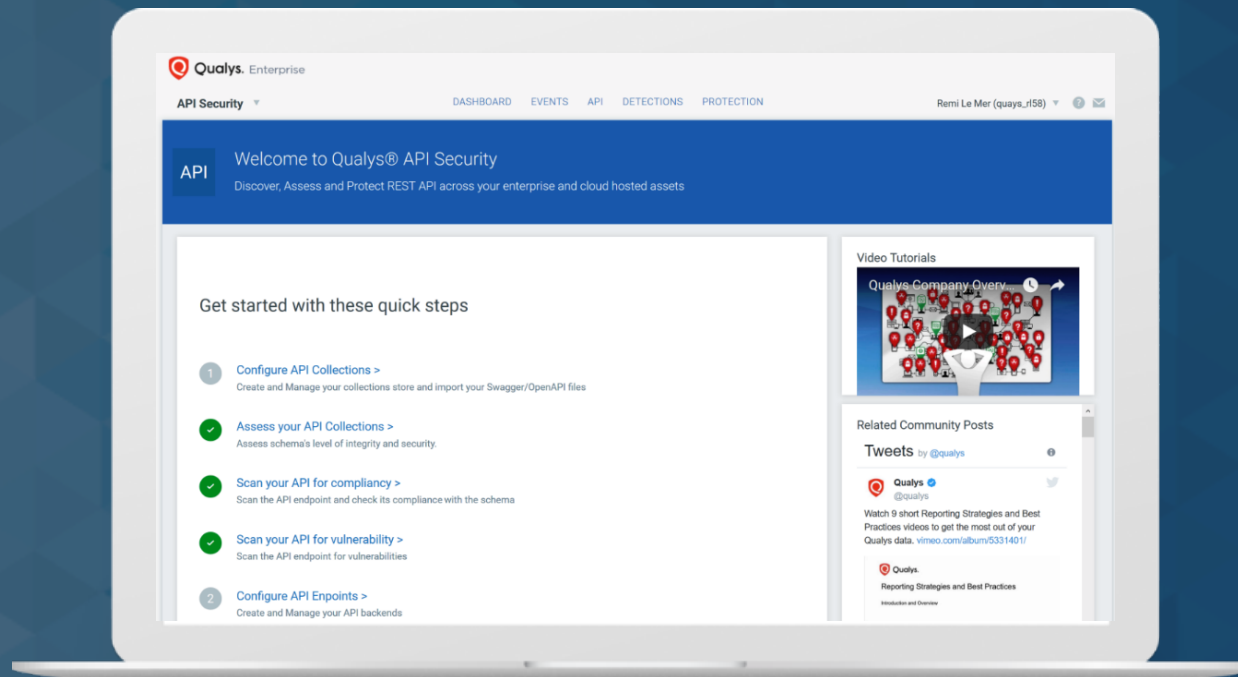
Qualys.

Qualys WAS Burp extension

WAS Enhancements, YTD

2018 | **2019**

April 2018
Swagger
Jenkins plugin
Qualys Browser
Recorder
Test Authentication
Exclude parameters

June 2018
SSTI
Header injection
WebLogic RCE
RichFaces RCE
"Spring Break"

Sept 2018
Browser engine
upgrade
XSS Power Mode
Tag apps upon import
ESI injection
WebSocket detection
PrimeFaces RCE

Jan 2018
CMS vulns
Multi-scan alerts
Update QID
mappings to 2017
OWASP Top 10

May 2018
Added CSV v2
report
Add'l CMS vulns

July 2018
Burp extension
Results for cancelled scans
Improved scan status
Scan settings snapshot
Retest multiple findings

Oct 2018
Blueimp file upload
Telerik crypto flaw

Qualys.

Qualys WAS Roadmap

WAS Roadmap

2018 | 2019

Feb-Mar 2019
TLS 1.3 support
SSL/TLS detections
Out-of-band detections
Security header tests
Enhanced crawling
CyberArk PIM integration

Dec 2018
Blind XPATH injection
Improved KB search
Custom report footer
Burp & Bugcrowd findings added to report
Ignore finding time limit
"Launch Now" for scheduled report

Jan 2019
Custom scan intensity
Jenkins plugin v2

Q2-Q3 2019
Elasticsearch
New dashboard
UI modernization
Support OpenAPI v3
Support Postman Collections

Qualys.

And Coming in 2019

Web Application Firewall

Review

Qualys WAF

Integration with WAS
Architecture improvements
Integration with Docker
Security Improvements
Roadmap – standalone
Roadmap – Integrated Suite

Qualys.
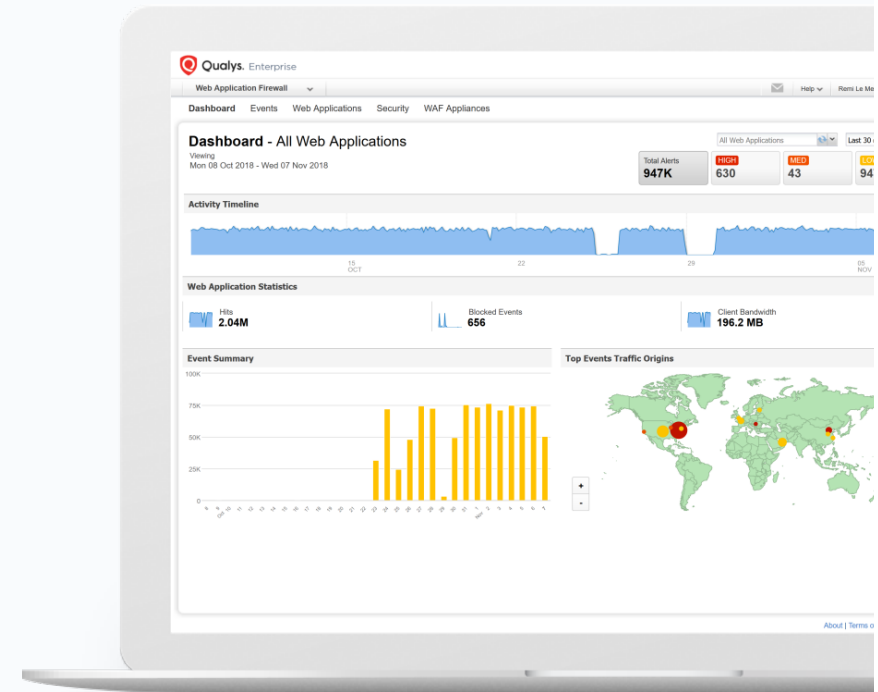
WAS / WAF Integration: ScanTrust

ScanTrust : Challenge your WAF protection

Assess both the application and the policy that protects it

WAS / WAF Integration: Virtual Patch

Virtual Patch : One-click mitigation tool for CISO teams

Run from within WAS to address confirmed threats

What's New in Qualys WAF

Supported Platforms

Shared and Private

Qualys Cloud Platforms

Add New WAF Appliance

Select Virtual Appliance Image

Choose the virtualization platform you want to use to run your WAF appliance on.

Platform		Details
⦿	VMware Standard	**VMware virtualization platform**
○	Hyper-V	**Microsoft Hyper-V 5.1 virtualization platform**
○	Amazon EC2	**Amazon EC2-Classic, Amazon EC2-VPC**
○	Microsoft Azure	**Microsoft Azure platform**
○	Google Cloud	**Google Cloud platform**
○	Docker	**Docker platform**

Cancel   Previous   Continue

Qualys.

WAF Architecture Improvements

Easy and usable Architecture

Virtual Reverse-Proxy

Cluster-able within hybrid topologies

Load-Balancing capabilities

SSL/TLS cipher suite categories

Qualys.

WAF Architecture Improvements

Virtual Appliance & Container (v1.5.3)

XML/JSON content inspection

Docker Host integration for backend automation

Better performance

Scheduled upgrades

Orchestration via Qualys API

Qualys.

Docker

Single Host

Controls :
- containers (start | stop | delete | inspect)
- networks
- images (pull | push | delete)

docker CLI

docker

dockerd

registry
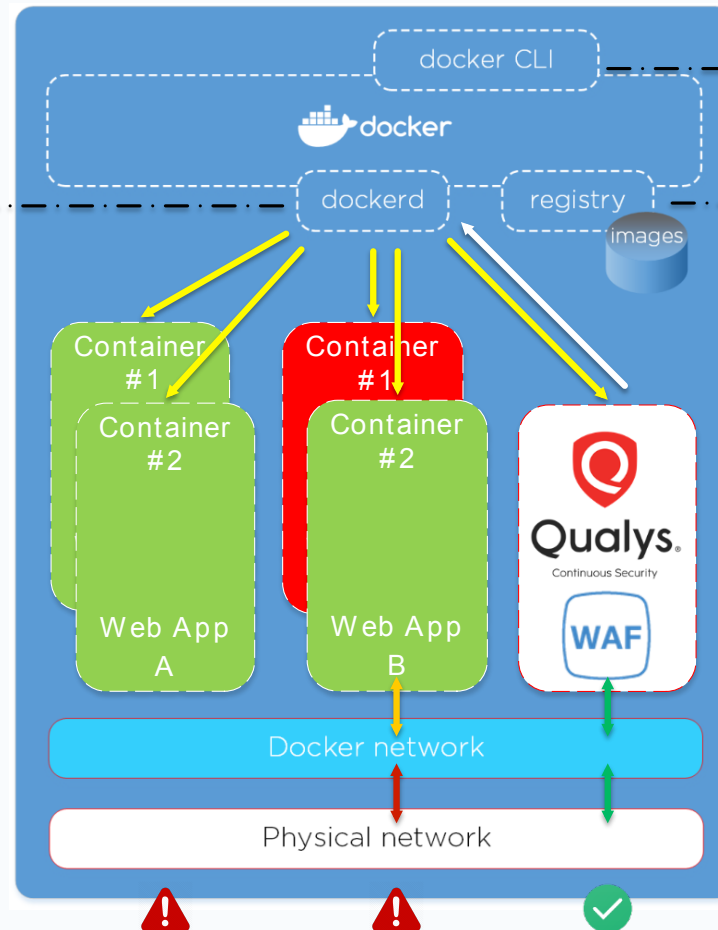
images

Access to docker services via unix sockets

Stores images

Container #1

Container #2

Web App A

Container #1

Container #2

Web App B

Qualys.
Continuous Security

WAF

Docker network

Physical network

Qualys.

Docker

Multiple Hosts

Access to docker services via network sockets

Host 1:
- docker CLI
- docker
- dockerd
- registry
- images

Container #1
Web App C

Docker network

Physical network

Host 2:
- docker CLI
- docker
- dockerd
- registry
- images

Container #1
Container #2
Web App A

Container #1
Container #2
Web App B

Docker network

Physical network

Qualys Virtual Firewall Appliance

Amazon EC², Azure, Google Hyper-V, VMWare

WAF

Physical network
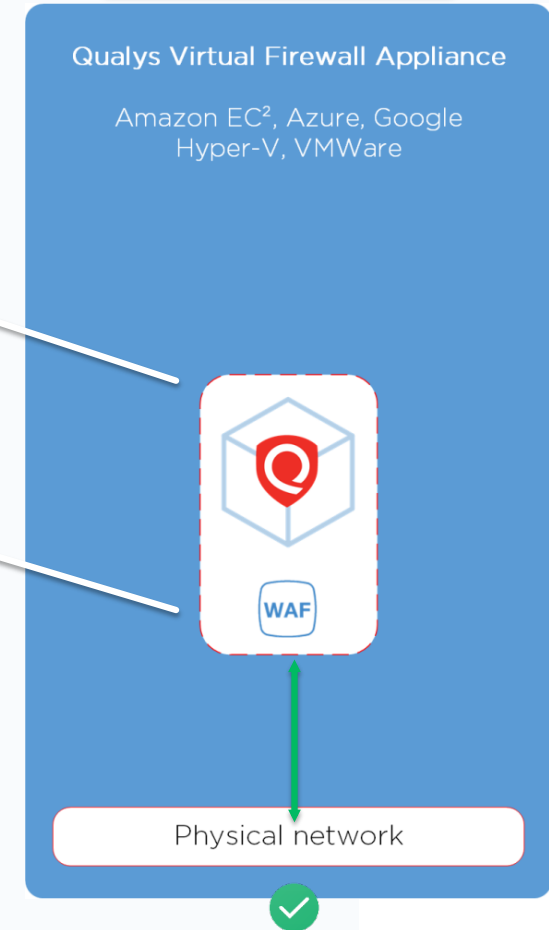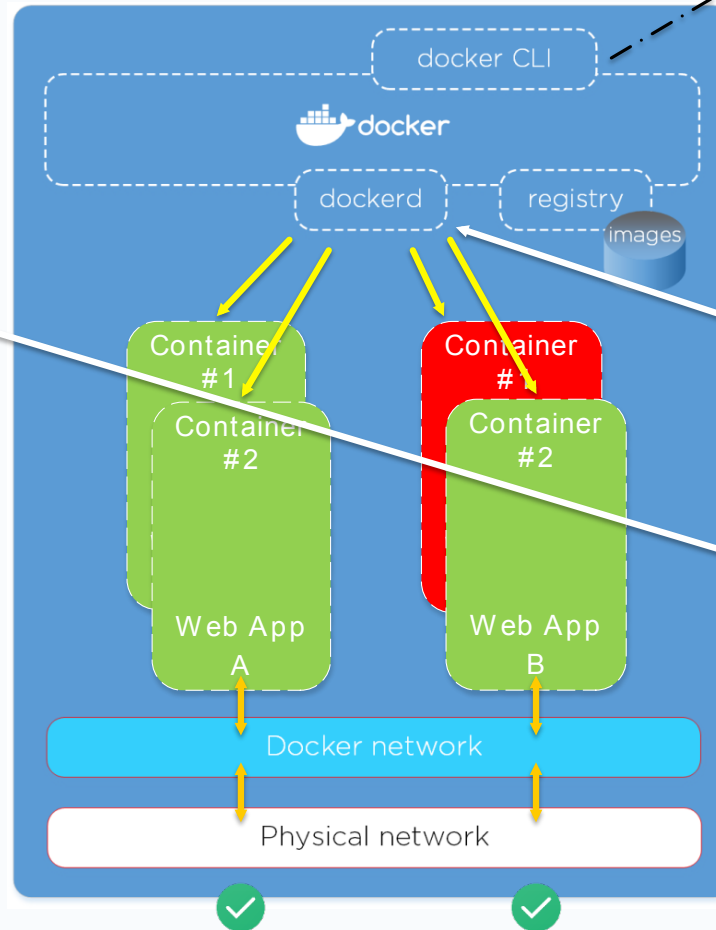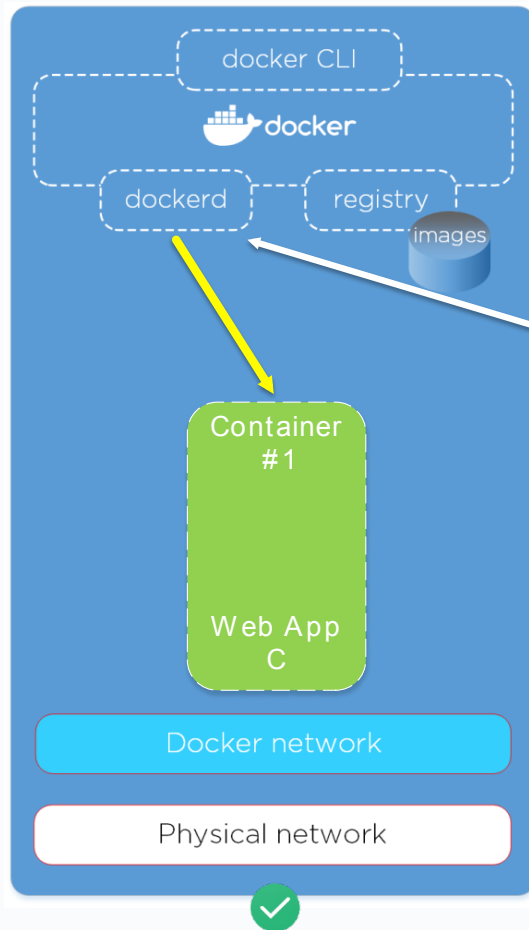
Security Improvements

Custom Rules: write and manage your own filters

- XML/JSON inspection
- Virtual Patches and Event Exceptions
- Latency control
- Rewriting capabilities (headers)

Qualys Rulesets and Templates

- DAG based inspection, programmable logic
- Drupal 8.0.x, Joomla 3.4.x, Magento 2.5-2.6, Wordpress 4.2.x-4.3.x
- JBoss 4.x-7.x, OWA 2010-2017, Sharepoint 2010-2017, Tomcat 8.0.x
- Qualys Generics for unknown apps

Qualys.

WAF Roadmap - Standalone

2018 | **2019**

Mar 2019
Templates
API Generics, Microsoft
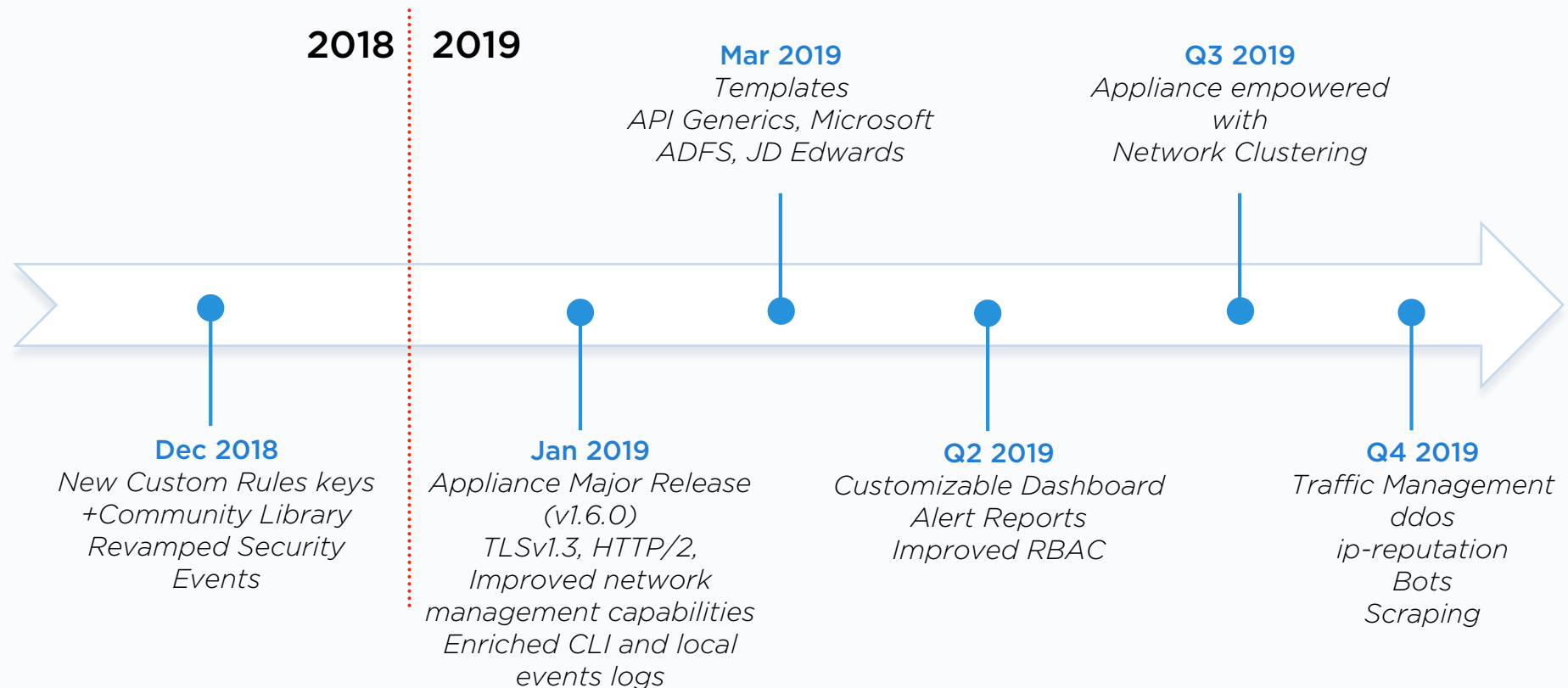*ADFS, JD Edwards*

Q3 2019
Appliance empowered
with
Network Clustering

Dec 2018
New Custom Rules keys
+Community Library
Revamped Security
Events

Jan 2019
Appliance Major Release
(v1.6.0)
TLSv1.3, HTTP/2,
Improved network
management capabilities
Enriched CLI and local
events logs

Q2 2019
Customizable Dashboard
Alert Reports
Improved RBAC

Q4 2019
Traffic Management
ddos
ip-reputation
Bots
Scraping

Qualys.

WAF Roadmap – Integrated Suite

2018 | **2019**

Mar 2019
WAS reports with ScanTrust details

Q3 2019
Virtual Patch supports Burp and Bug Bounties

Dec 2018
AI - Feed Application inventory with backend information

Jan 2019
UD – WAF widgets and queries

Q2 2019
App's Sitemap v2 (WAS & WAF)

ScanTrust enabled on VM

Q4 2019
CV - fetch app's grade and patch SSL implementation

Qualys.